

REMARKS

The present reply is responsive to the Office Action mailed October 17, 2005. Claims 1, 4-5, 13, 15-16, 19, 22-23, 29-33, 36, 40 and 46 have been amended. No new matter has been added by these amendments. Support for the amendments may be found, by way of example only, in specification paragraphs 0537 to 0563 and FIG. 22. Claims 47-101 and 137-178 were previously withdrawn from consideration and have been cancelled in the present amendment. Claims 2-3, 10-11, 17-18, 20-21, 27-28, 34-35, 37-38, 44-45 and 102-136 have also been cancelled. Therefore, claims 1, 4-9, 12-16, 19, 22-26, 29-33, 36, 39-43 and 46 are again presented for the Examiner's consideration. A petition for a one-month extension of time is respectfully submitted herewith.

As an initial matter, claim 130 was rejected under 35 U.S.C. § 112, first and second paragraphs. As claim 130 has been cancelled, these rejections have been mooted. The other rejections of the Office Action will be addressed with respect to the currently pending claims.

Claims 1, 7-8, 12, 19, 24-25, 29, 36, 41-42 and 46 have been rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 6,011,849 ("Orrin"). Applicants respectfully traverse the rejection.

The rejection cites to several portions of *Orrin* in rejecting independent claims 1, 19, 36 and 46. The first portion is entitled "Selective Text Encryption" and states "The system allows the user to highlight and select portions of the text, including paragraphs, sentences, even words, to be encrypted within a plaintext document. Delimiters are used so that a user decrypting the selected text does not have to identify its exact boundaries." (Col. 7, ll. 13-18.)

The next portion is entitled "Digital Signatures" and states "Digital Signatures--The system provides Digital Signature capability to its users. Digital Signatures verify the origin and document integrity using one way hash functions and the Signing key belonging to the user. The system generates a hash sequence based on the contents of a document and then encrypts it with the Signing key. This sequence can be checked by the recipient to validate the sender and the contents of the document by decrypting the hash sequence using the verification key, packaged with the user's public key, and then comparing the hash of the document to the one contained in the Digital Signature. Digital Signatures can be used on both plaintext as well as ciphertext messages." (Col. 7, ll. 30-41.)

The final section relates to secure backup on removable media, and states "At step 39 the encrypted data is split into files corresponding to the number of removable media to be used. This splitting function involves taking bytes from the encrypted data and placing them into separate files such that each byte is placed in a different file than its adjacent bytes. For example, if three files were to be created using the splitting process in step 39, and 'abedefghijklmno' was the starting file to be stored, the resulting split files would be: 'adgjm', 'behkn', and 'cfilo'. This process eliminates unwanted exposure of partial ciphertexts in the event that the security of one or more of the split files is compromised. In step 40, each split file is written to selected sectors of its removable media. The key produced in step 37 is used to choose the exact sector(s) on the removable media where the files are written." (Col. 8, ll. 53-67.)

However, neither these nor any other portions of *Orrin* teach or suggest the limitations of any of the independent claims. By way of example only, with regard to claim 1, *Orrin* does not teach, suggest or otherwise disclose a cryptography

process section that "generates first integrity check values as integrity check values for a message including a usage policy obtained by a header of said content data, collates said first integrity check values to verify said message, generates second integrity check values as integrity check values for information including at least a content key obtained by said header of said content data, collates said second integrity check values to verify said information, generates an intermediate integrity check value based on said first integrity check values and said second integrity check values, and uses said intermediate integrity check value to verify said content data corresponding to said first and second integrity check values."

With regard to claim 19, there is no teaching or suggestion of performing a method including "generating first integrity check values as integrity check values for a message including a usage policy obtained by a header of said content data; collating said first integrity check values to verify said message; generating second integrity check values as integrity check values for information including at least a content key obtained by said header of said content data; collating said second integrity check values to verify said information; generating an intermediate integrity check value based on said first integrity check values and said second integrity check values; and verifying said content data corresponding to said first and second integrity check values using said intermediate integrity check value."

With regard to claim 36, there is likewise no teaching or suggestion of performing a method including "imparting first integrity check values as integrity check values for a message including a usage policy obtained by a header of content data; imparting second integrity check values as integrity check values for information including at least a content key obtained by said header of said content data; and imparting an

intermediate integrity check value to data to be verified, said intermediate integrity check value being used to verify content data corresponding to said first integrity check values and said second integrity check values."

Finally, with regard to claim 46, *Orrin* does not teach or otherwise suggest "a recording medium recorded with a computer program for executing a data verifying process having certain actions, said actions comprising: executing a collation process using first integrity check values generated as integrity check values for a message including a usage policy obtained by a header of content data; executing a collation process using second integrity check values generated as integrity check values for information including at least a content key obtained by said header of said content data; and using an intermediate integrity check value to verify said content data corresponding to said first and second integrity check values, said intermediate integrity check value being based on an integrity check value set obtained by combining at least some of said first and second integrity check values together."

None of the art of record remedies the deficiencies of *Orrin*. For at least this reason, applicants respectfully submit that the rejection of independent claims 1, 19, 36 and 46 should be withdrawn. Claims 7-8, 12, 24-25, 29, and 41-42 depend from claims 1, 19 and 36, respectively, and contain all of the limitations thereof as well as other limitations that are neither disclosed nor suggested by the prior art of record. Accordingly, applicants submit that these dependent claims are likewise patentable.

Claims 4-6, 22-23 and 39-40 were rejected under 35 U.S.C. § 103(a) as being obvious over *Orrin* in view of U.S. Patent No. 6,898,709 ("*Teppler*"). Claims 9, 26 and 43 were rejected under 35 U.S.C. § 103(a) as being obvious over *Orrin* in

view of U.S. Patent No. 6,915,434 ("Kuroda"). Claims 13-15 and 30-32 were rejected under 35 U.S.C. § 103(a) as being obvious over Orrin in view of U.S. Patent No. 5,680,587 ("Bodo"). And claims 16 and 33 were rejected under 35 U.S.C. § 103(a) as being obvious over Orrin in view of Bodo and U.S. Patent No. 6,055,236 ("Nessett").


Claims 4-6, 9, 13-16, 22-23, 26, 30-33, 39-40 and 43 depend from claims 1, 19 and 36, respectively, and contain all of the limitations thereof as well as other limitations that are neither disclosed nor suggested by the prior art of record. Accordingly, applicants submit that these dependent claims are likewise patentable.

As it is believed that all of the rejections set forth in the Office Action have been fully met, favorable reconsideration and allowance are earnestly solicited.

If, however, for any reason the Examiner does not believe that such action can be taken at this time, it is respectfully requested that he telephone applicant's attorney at (908) 654-5000 in order to overcome any additional objections which he might have. If there are any additional charges in connection with this requested amendment, the Examiner is authorized to charge Deposit Account No. 12-1095 therefor.

Dated: February 17, 2006

Respectfully submitted,

By 
Andrew T. Zidel
Registration No.: 45,256
LERNER, DAVID, LITTENBERG,
KRUMHOLZ & MENTLIK, LLP
600 South Avenue West
Westfield, New Jersey 07090
(908) 654-5000
Attorney for Applicant